Empowering Network Processors

DeepSweep™ Tutorial

Single-port

'T1_IAS' Example

June 2007

IP Fabrics, Inc.
14964 NW Greenbrier Parkway
Beaverton, OR 97006
503-444-2400
503-444-2401 FAX
www.ipfabrics.com

Introduction

This document is a simple step by step tutorial that guides you through the stages involved to construct a sample DeepSweep™ IAS example. This example employs a system with a single Packet Inspection Accelerators (PIXL) that is resident on one Double Espresso (DE) board. This provides dual Gbit Ethernet ports.

Let's set up the sample scenario. We want to capture both identifying information and content for a particular subject. We know the MAC address and some other identifying information. In this sample system, IP addresses are sometimes fixed and sometimes assigned by DHCP.

Figure 1 depicts a greatly simplified network topology for this example. The purpose of this tutorial is to go though the DeepSweep concepts rather than how to set up an ISP. It shows the use of a method to provide all packets in a single simplex Ethernet stream. Specifically, this single stream will contain DHCP "controller" input and all of "content." This can be done in a variety of ways such as mirror/span port, or an aggregating tap. This is highly installation dependent.

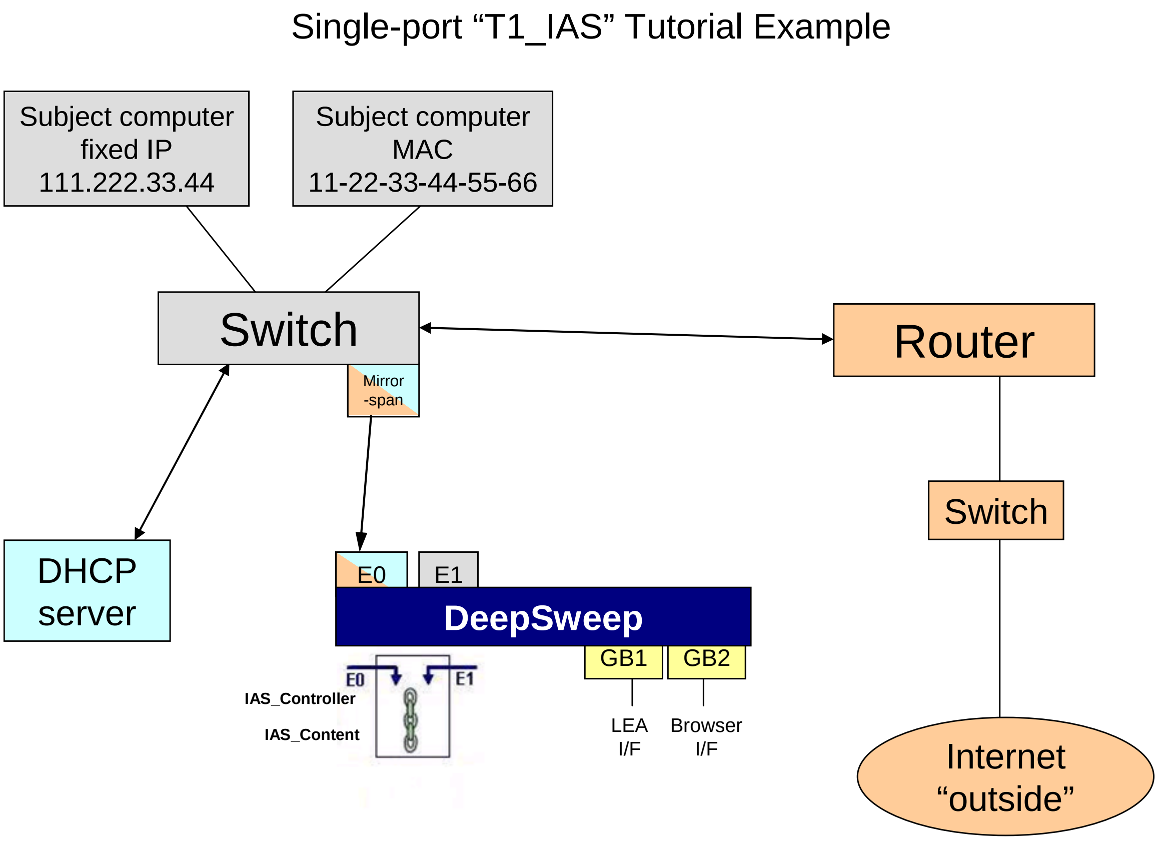


Figure 1. "T1_IAS" simplified network example

We will use one DeepSweep port to watch all DHCP assignments and content traffic. One system port (GB1 in this example) is connected to the network so that a browser has access to the DeepSweep and the other system port (GB2) must have access to a path to the 'collector' system of the LEA. Of course, these could be the same interfaces if one wishes. Again, this is highly installation dependent. In this example, we assume that these connections and associated configuration have already been done.

A step-by-step tutorial follows. At a high level, the process is:

1. Open a browser to DeepSweep
2. Log in
3. Define two Surveillance Modules (SM) – one to watch control information and one to watch content.
4. Define a Surveillance Assembly (SA).
5. Start the SA.
6. Re-examine the IAS Controller once the system is running
7. Stop the running SA.

"T1_IAS" Step-by-step Instructions

Step 1: Point browser to configuration screens

Point your browser to the DeepSweep login screen. Use HTTPS with the IP address of the DeepSweep. Systems have been tested with Microsoft IE and Mozilla Firefox browsers. If the DeepSweep IP address has been set to 192.168.43.50 then one would enter the URL as:

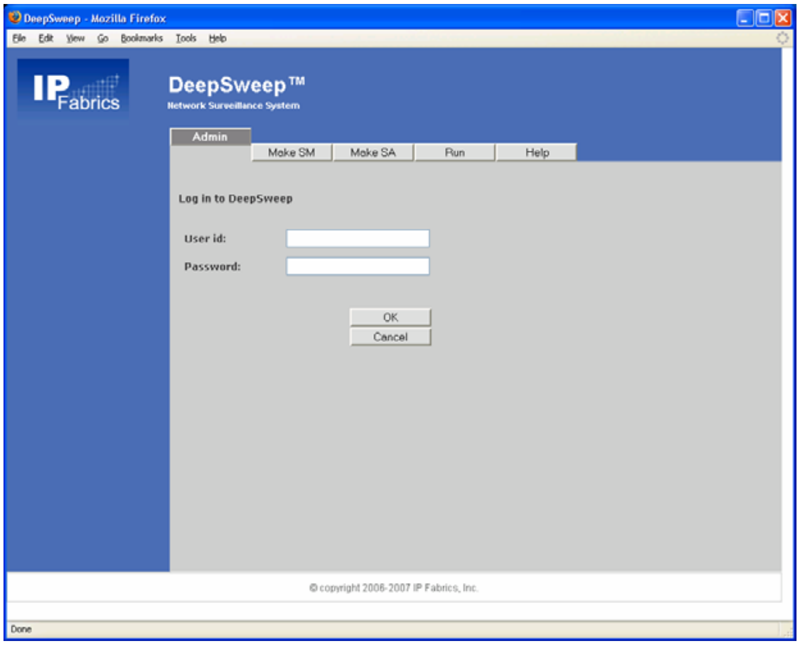
https://192.168.43.50

If you are running the DeepSweep with a locally attached display, keyboard and mouse then use:

http://127.0.0.1

Step 2: Login

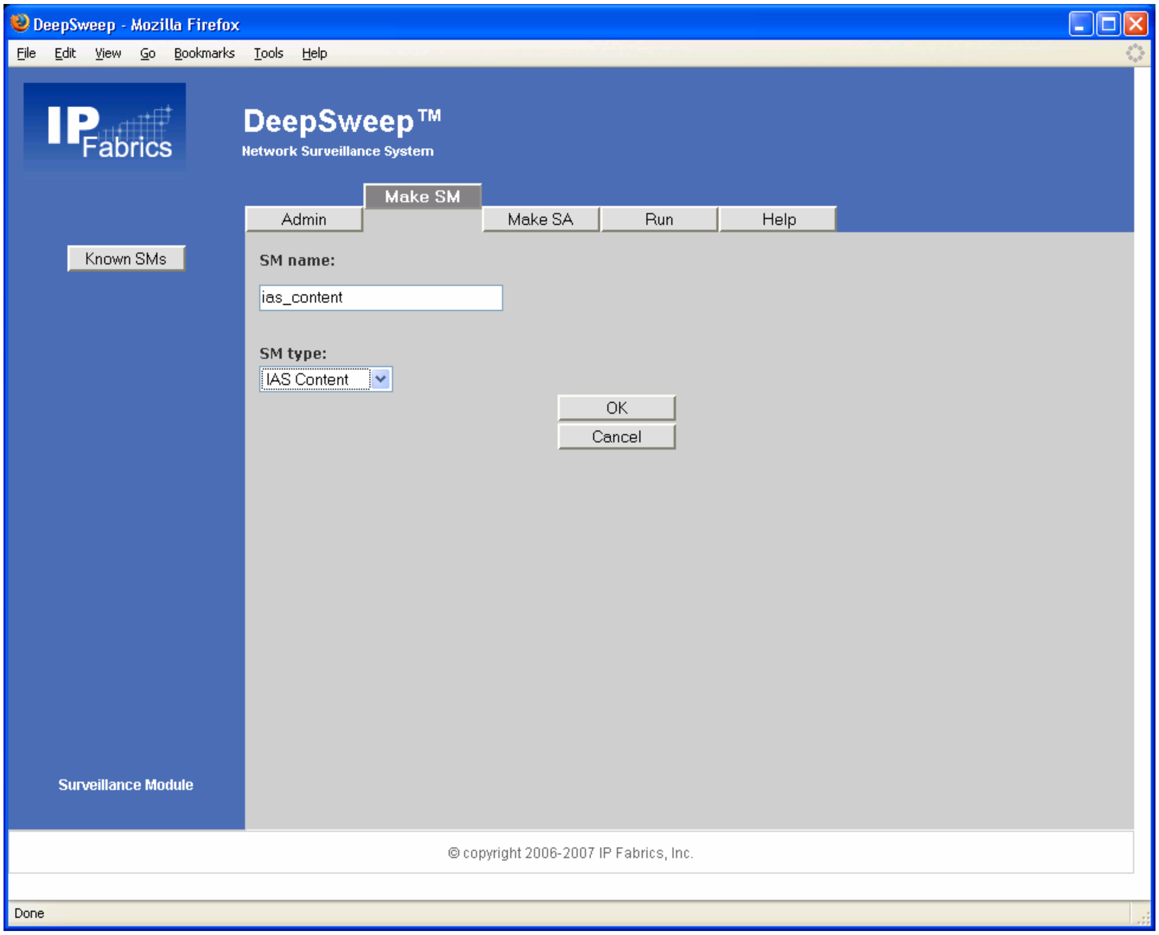
If you have set up a user account already then do use it to log in. If you have not yet set up a user account then use 'admin' account with the default (as shipped) password 'ipfabrics'. These are all lower case. You can set up your own account later by following the instructions in the user manual. Note that some screens may be different for "admin" vs. a non-admin user name.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Admin
Make SM
Make SA
Run
Help
Log in to DeepSweep
User id:
Password:
OK
Cancel
© copyright 2006-2007 IP Fabrics, Inc.
Done

Step 3: Define ‘ias_content’ Surveillance Module (SM)

This is the first of two Surveillance Modules (SM) you will need to define for the tutorial. This SM will be of type IAS Content and will be watching the content packet stream.

1. Click ‘Make SM’ tab.
2. Click ‘New’ button.
3. Select ‘IAS Content’ from the ‘SM type’ menu.
4. Click in blank box labeled ’SM name’.
5. Enter the string ’ias_content’
6. Click OK button.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Make SM
Admin
Make SA
Run
Help
Known SMs
OK
Cancel
Surveillance Module
© copyright 2006-2007 IP Fabrics, Inc.
Done

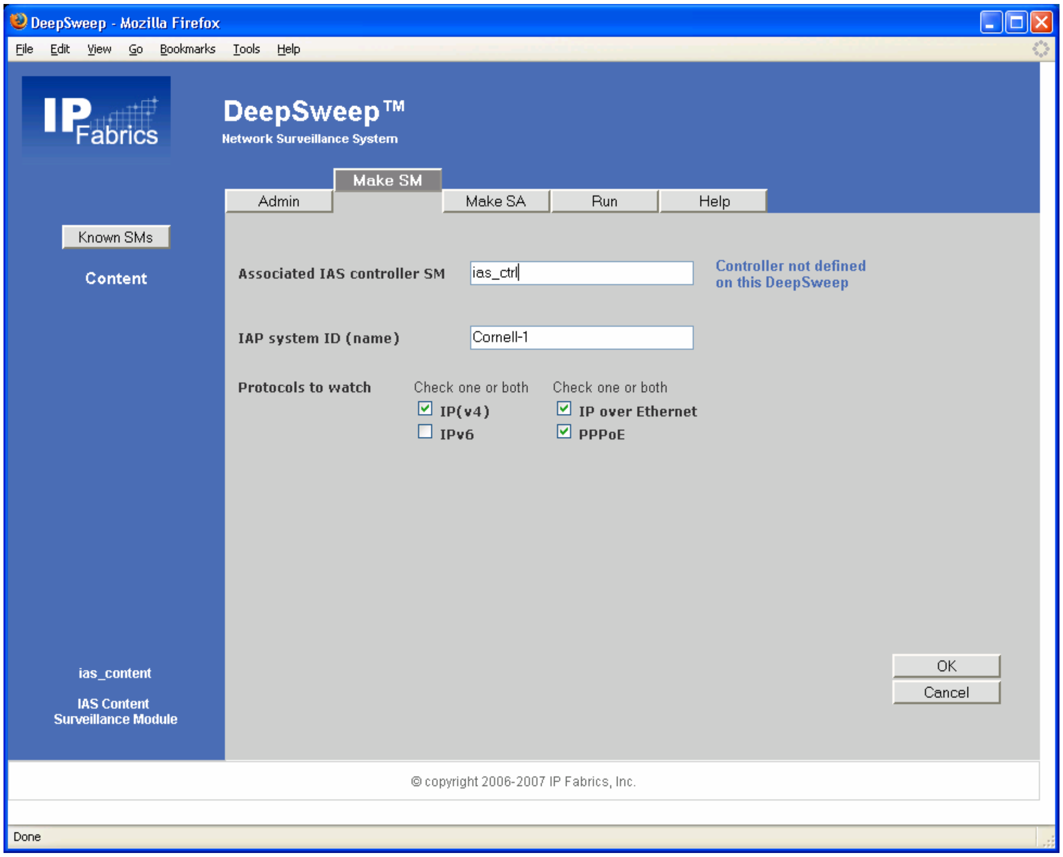
SM name: ias_content

SM type: IAS Content

This takes you to the configuration page for this SM type.

Now we will configure the IAS Content SM with the specific criteria this specific SM will use. There is only a single configuration screen for this SM type.

7. Enter “ias_ctrl” as the associated IAS controller. This SM name does not exist in the system since we have not defined it yet. That is OK. We will do that next. When we are done this name must match the name of the IAS controller from which IAS content SM will listen for its instructions.
8. Enter “Cornell-1” as the IAP system ID. This can be any identifying string you desire and will be reported in some of the T1.IAS messages to an LEA collector software system.
9. Leave the other check boxes as they are shown here.
10. Click OK.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Admin
Make SM
Make SA
Run
Help
Known SMs
Content
ias_content
IAS Content Surveillance Module
OK
Cancel
© copyright 2006-2007 IP Fabrics, Inc.
Done

Associated IAS controller SM: ias_ctrl

Controller not defined on this DeepSweep

IAP system ID (name): Cornell-1

Protocols to watch

Check one or both
☑ IP(v4)
□ IPv6

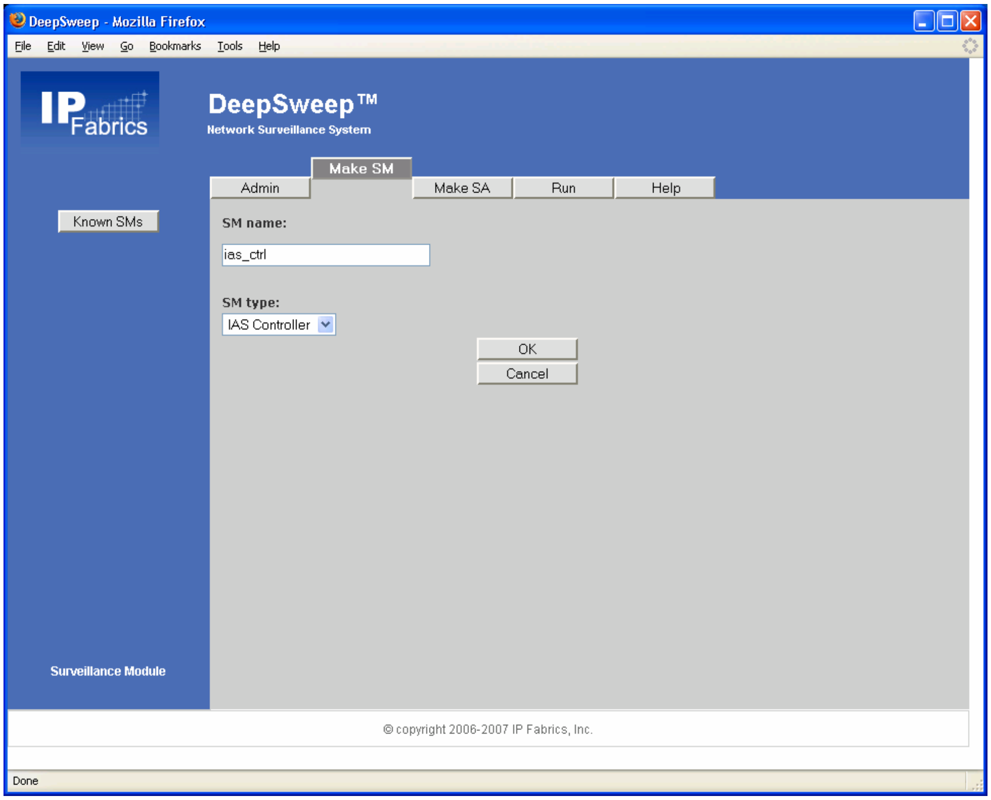
Check one or both
☑ IP over Ethernet
☑ PPPoE

This completes the configuration of the IAS Content SM.

Step 4: Define 'ias_ctrl' Surveillance Module

Create the second SM which will be named 'ias_ctrl'. This will be a different type of SM – IAS Controller – but the process is similar.

1. Click 'Make SM' tab.
2. Click 'New' button.
3. Select 'IAS Controller' from the 'SM type' menu.
4. Click in blank box labeled 'SM name'.
5. Enter the string 'ias_ctrl'
6. Click OK button.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Make SM
Admin
Make SA
Run
Help
Known SMs
OK
Cancel
Surveillance Module
© copyright 2006-2007 IP Fabrics, Inc.
Done

SM name:

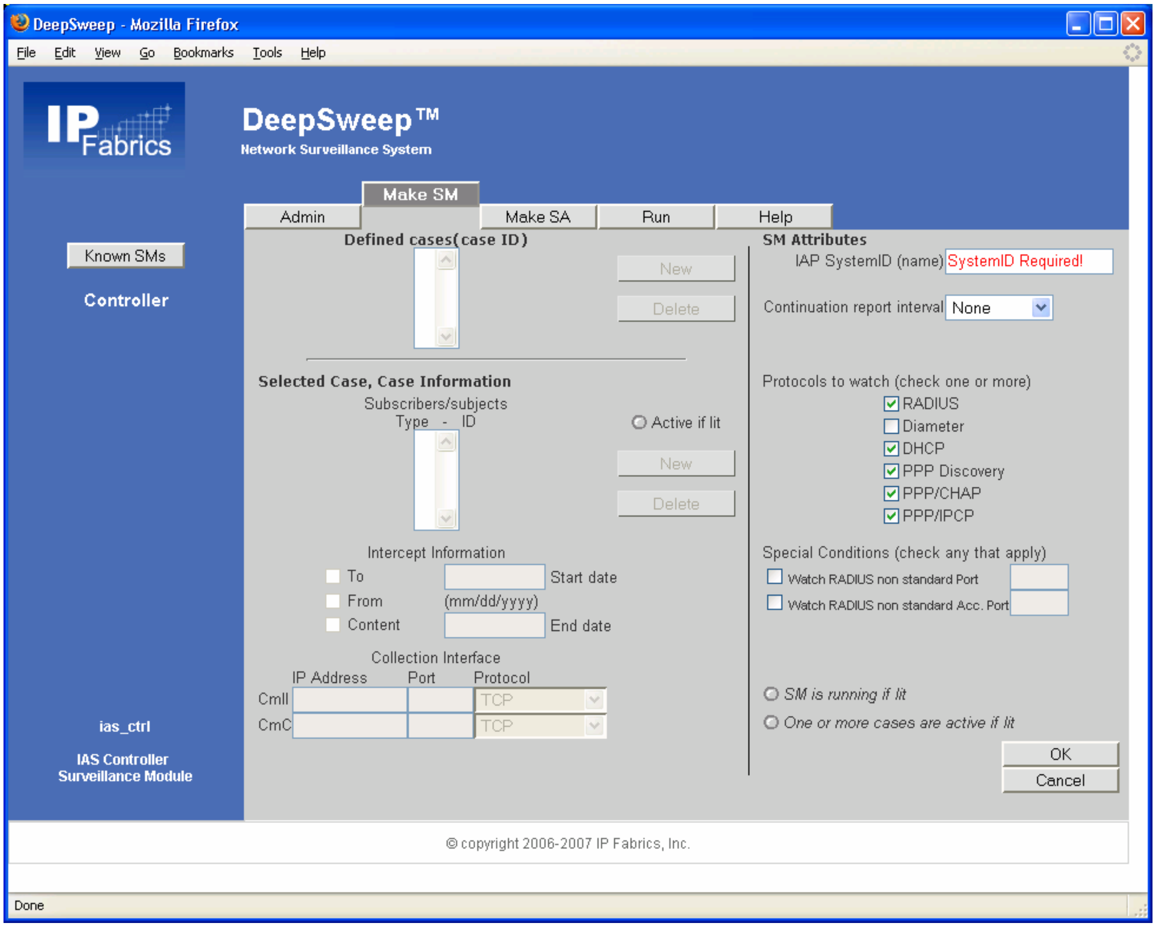
ias_ctrl

SM type:

IAS Controller

This takes you to the configuration page for this SM type.

There is a single setup screen for this SM definition. Initially, this screen will be as below.



Defined cases(case ID)

Selected Case, Case Information

Subscribers/subjects

Type - ID

○ Active if lit

Intercept Information

□ To Start date

□ From (mm/dd/yyyy)

□ Content End date

Collection Interface

	IP Address	Port	Protocol
CmII			TCP
CmC			TCP

SM Attributes

IAP SystemID (name) SystemID Required!

Continuation report interval None

Protocols to watch (check one or more)

☑ RADIUS
□ Diameter
☑ DHCP
☑ PPP Discovery
☑ PPP/CHAP
☑ PPP/IPCP

Special Conditions (check any that apply)

□ Watch RADIUS non standard Port

□ Watch RADIUS non standard Acc. Port

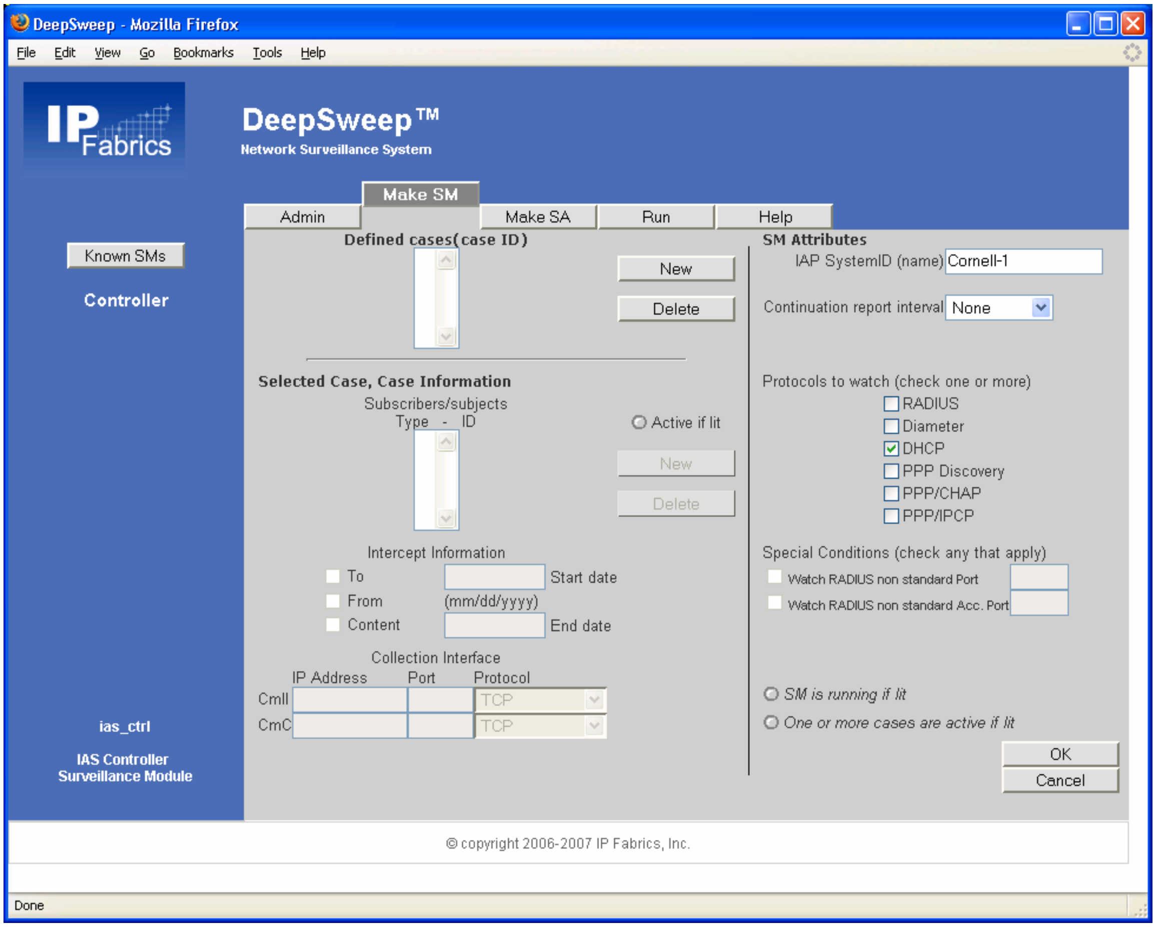
○ *SM is running if lit*

○ *One or more cases are active if lit*

© copyright 2006-2007 IP Fabrics, Inc.

First, we will enter the SM Attributes information. This is the information on the right side of the page.

7. Enter “Cornell-1” as the IAP system ID. Same as in the other SM definition.
8. Check/uncheck the protocol boxes so as to leave only DHCP to watch. It would be acceptable to check the other protocol boxes, too, but we leave them unchecked since we know we only care about DHCP in this example.
9. Click OK.



SM Attributes

IAP SystemID (name) Cornell-1

Continuation report interval None

Protocols to watch (check one or more)

□ RADIUS
□ Diameter
☑ DHCP
□ PPP Discovery
□ PPP/CHAP
□ PPP/IPCP

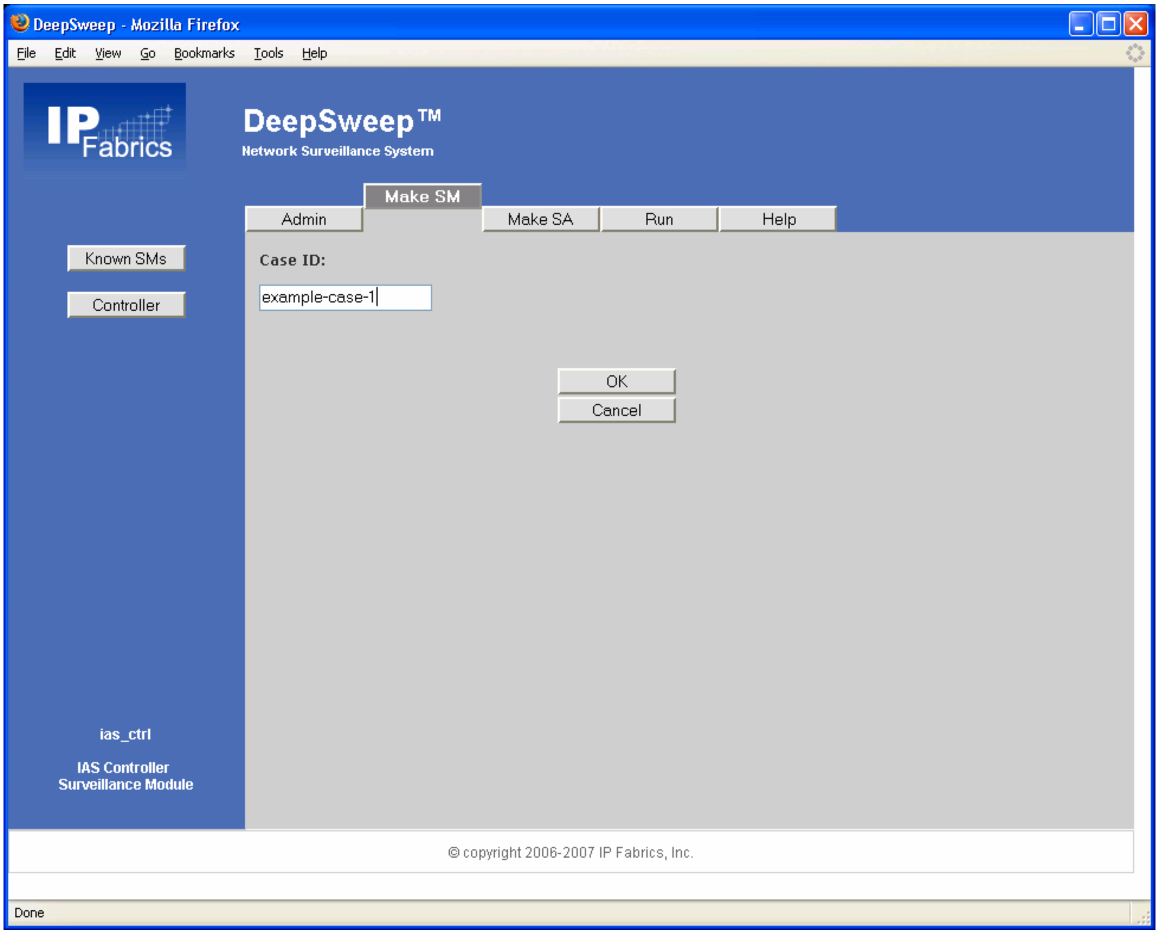
Special Conditions (check any that apply)

□ Watch RADIUS non standard Port
□ Watch RADIUS non standard Acc. Port

○ SM is running if lit
○ One or more cases are active if lit

Next we will define a new case.

10. Click "New" button that is near the case section of the page. This takes you to a simple screen with a single text-entry box..
11. Enter "example-case-1" in the text box.
12. Click OK.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Make SM
Admin
Make SA
Run
Help
Known SMs
Controller
OK
Cancel
ias_ctrl
IAS Controller
Surveillance Module
© copyright 2006-2007 IP Fabrics, Inc.
Done

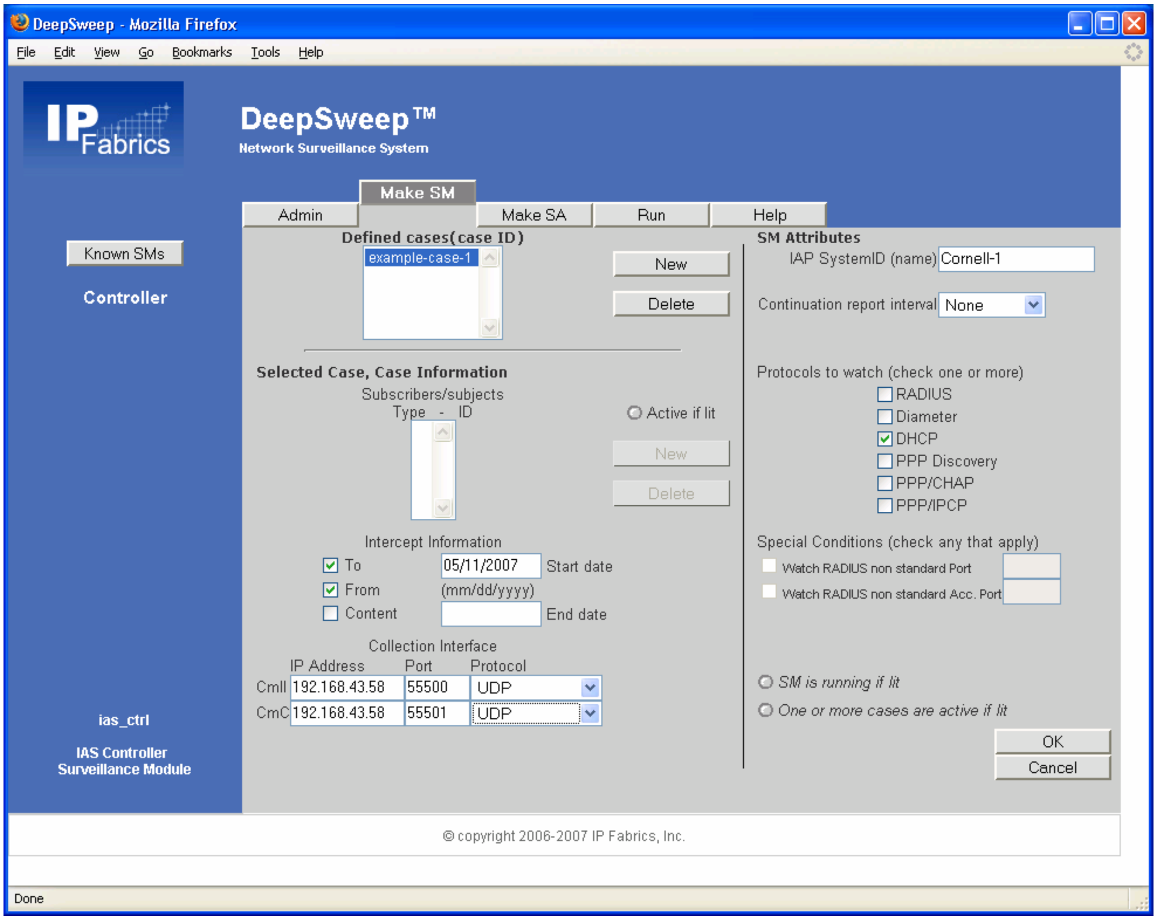
Case ID: example-case-1

You will be returned to the IAS Controller definition page.

Now we will define the parameters for this sample case.

13. Make sure the newly added case name is highlighted. If it is not then click on the name.
14. Check the intercept information boxes for To, From and Content.

    Note that the start date should be today's date and the end date will be blank. Just leave them that way. If the start date is not correct then confirm that your system's time zone is set correctly and (possibly) that you have a valid path to an NTP time server. See the *DeepSweep User's Manual* for more information if this is not set up properly.
15. Enter your own 'safe' IP address, port number and protocol for both Collection Interfaces – CmII and CmC. Be sure to select UDP since there is no actual live LEA collector at the receiving side of this example. These are for "Communications Identifying Information" and "Communications Content." If you really want to examine the output then these need to be valid IP and port entries. They need not be valid to run through the example but, if you have the LEA port connected to your network, then you should make sure this traffic would not cause a problem.
16. Click OK.



Defined cases(case ID): example-case-1

SM Attributes

IAP SystemID (name): Cornell-1

Continuation report interval: None

Selected Case, Case Information

Subscribers/subjects Type - ID

○ Active if lit

Protocols to watch (check one or more)

□ RADIUS
□ Diameter
☑ DHCP
□ PPP Discovery
□ PPP/CHAP
□ PPP/IPCP

Intercept Information

☑ To
☑ From
□ Content

Start date (mm/dd/yyyy): 05/11/2007

End date:

Special Conditions (check any that apply)

□ Watch RADIUS non standard Port
□ Watch RADIUS non standard Acc. Port

Collection Interface

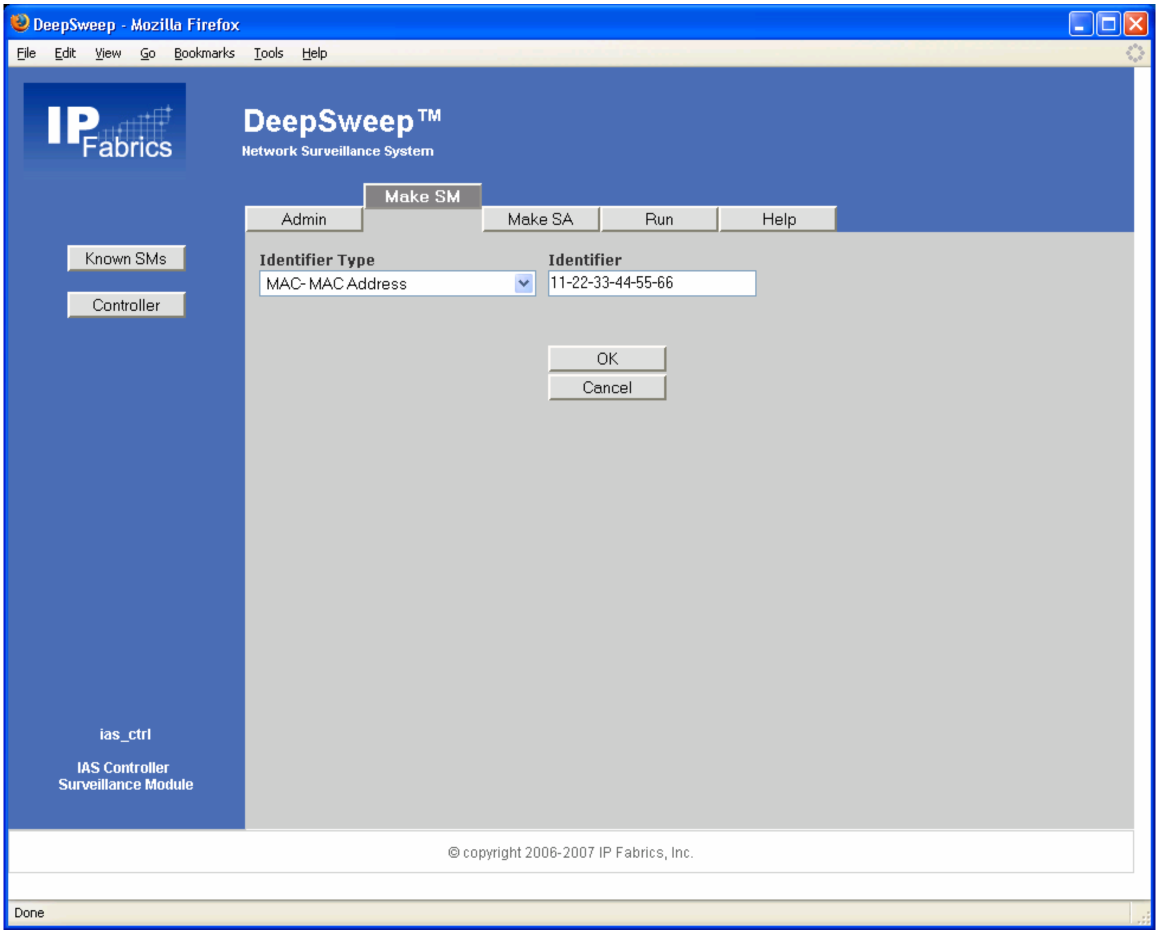
	IP Address	Port	Protocol
CmII	192.168.43.58	55500	UDP
CmC	192.168.43.58	55501	UDP

○ SM is running if lit

○ One or more cases are active if lit

Next we will make several subject ID entries for this case. In this example case, we will watch for DHCP assigning an IP address to a known MAC address. We will watch a known, fixed IP address.

17. Click on the "New" button in the middle of the IAS Controller page near the text "Selected Case, Case Information". This takes you to a screen for entry of Subject Identifiers.
18. Select MAC as Identifier Type and enter a MAC address. We use "11-22-33-44-55-66" in the example.
19. Click OK.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Admin
Make SM
Make SA
Run
Help
Known SMs
Controller
OK
Cancel
ias_ctrl
IAS Controller
Surveillance Module
© copyright 2006-2007 IP Fabrics, Inc.
Done

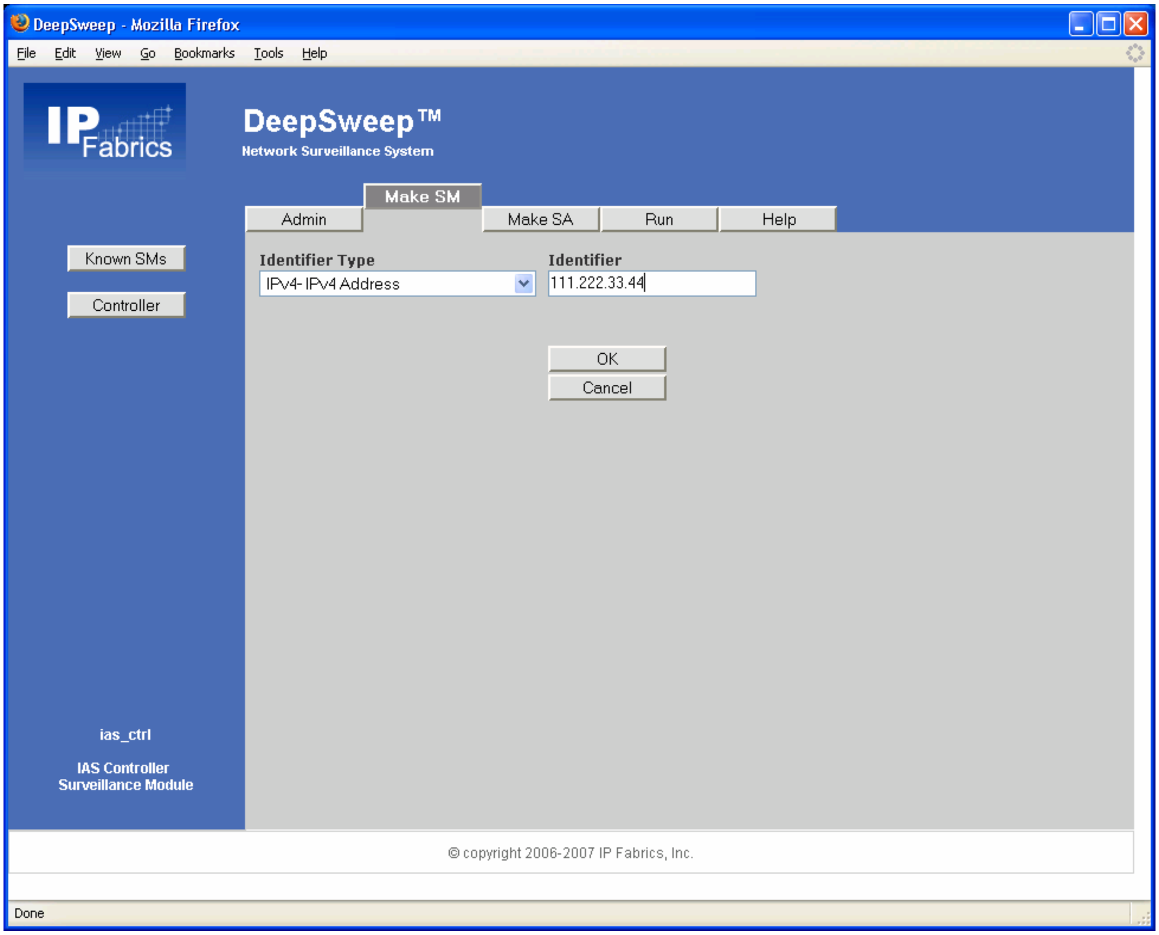
Identifier Type: MAC- MAC Address

Identifier: 11-22-33-44-55-66

This returns you to the IAS Controller configuration page.

Using the same process, add another Subject ID – the fixed IP address.

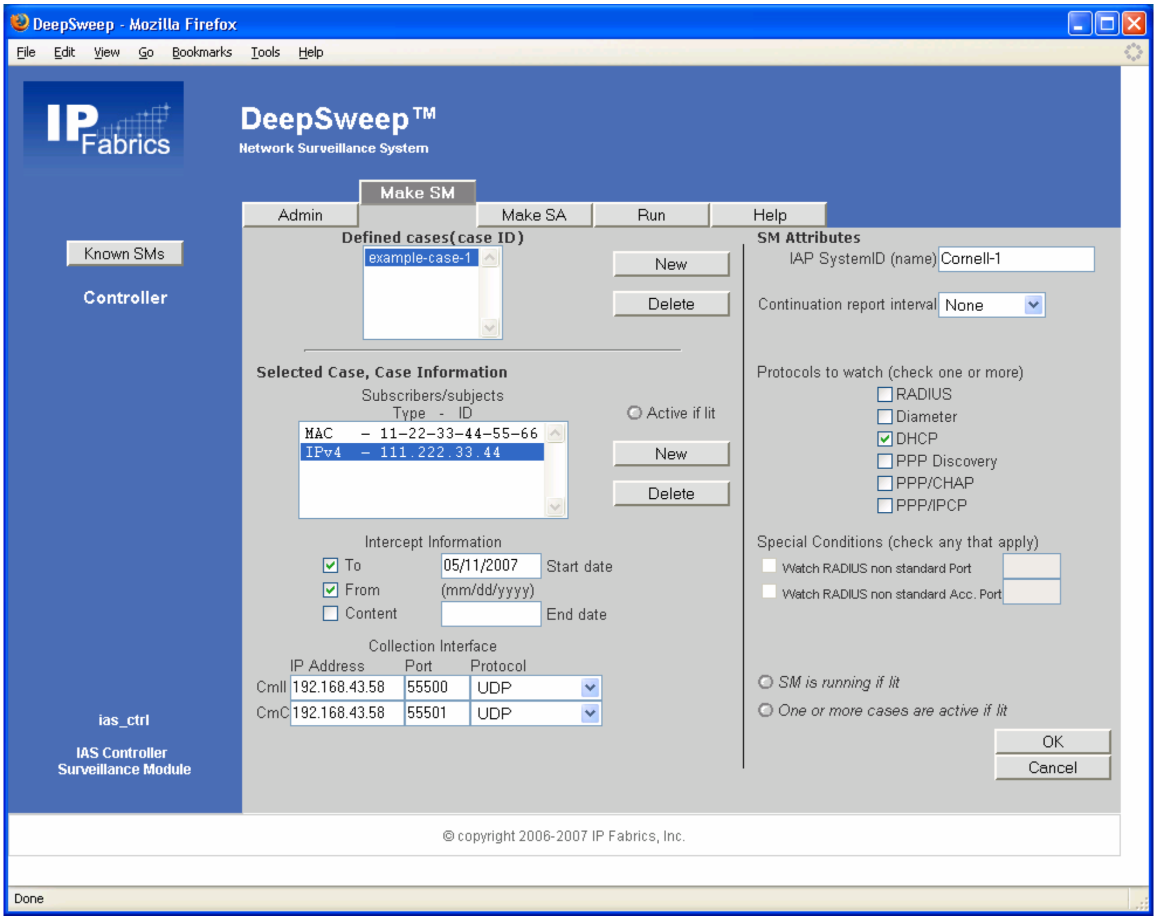
20. Click "New" for another new Subject ID.
21. Select IPv4 Identifier Type.
22. Enter "111.222.33.44" for this example.
23. Click OK.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Make SM
Admin
Make SA
Run
Help
Known SMs
Controller
OK
Cancel
ias_ctrl
IAS Controller
Surveillance Module
© copyright 2006-2007 IP Fabrics, Inc.
Done

Identifier Type: IPv4- IPv4 Address
Identifier: 111.222.33.44

You are returned to the IAS Controller configuration page.

This is how the page should now appear.



Defined cases(case ID)

example-case-1

Selected Case, Case Information

Subscribers/subjects

Type	ID
MAC	11-22-33-44-55-66
IPv4	111.222.33.44

○ Active if lit

Intercept Information

☑ To 05/11/2007 Start date
☑ From (mm/dd/yyyy)
☐ Content End date

Collection Interface

	IP Address	Port	Protocol
CmII	192.168.43.58	55500	UDP
CmC	192.168.43.58	55501	UDP

SM Attributes

IAP SystemID (name) Cornell-1

Continuation report interval None

Protocols to watch (check one or more)

☐ RADIUS
☐ Diameter
☑ DHCP
☐ PPP Discovery
☐ PPP/CHAP
☐ PPP/IPCP

Special Conditions (check any that apply)

☐ Watch RADIUS non standard Port
☐ Watch RADIUS non standard Acc. Port

○ *SM is running if lit*
○ *One or more cases are active if lit*

© copyright 2006-2007 IP Fabrics, Inc.

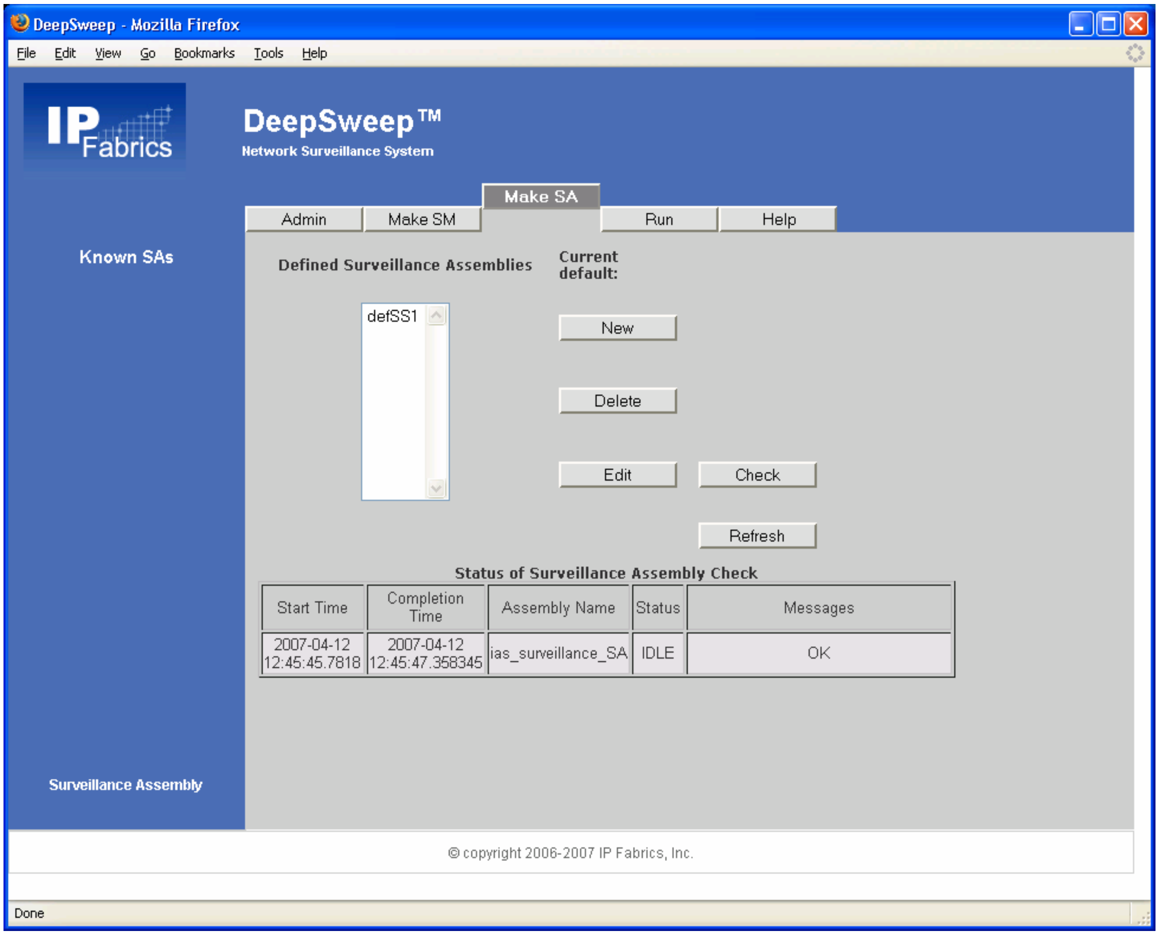
We are done defining the information for the IAS Controller SM – one case with two subject IDs.

Step 5: Construct 'ias_surveillance_SA' Surveillance Assembly

In this step we will construct the Surveillance Assembly (SA) that combines the two Surveillance Modules (SMs) that we just defined into a system of instances and interconnections. For this SA, we will take packets arriving at port E0 to be input to both the IAS Controller SM and IAS Content SM. We will do nothing with packets on the other interfaces.

We begin by defining a new SA named 'ias_surveillance_SA'.

1. Click on 'Make SA' tab.

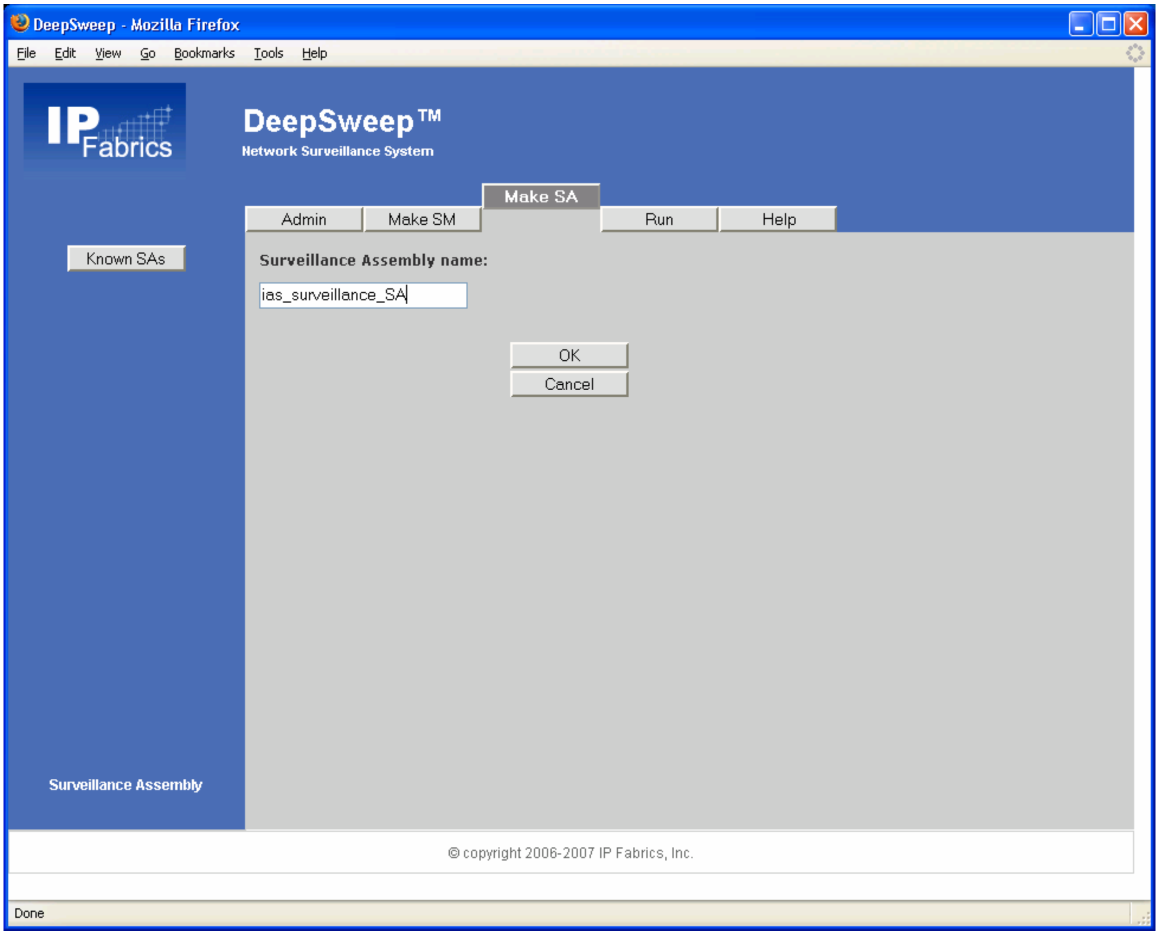


Status of Surveillance Assembly Check

Start Time	Completion Time	Assembly Name	Status	Messages
2007-04-12 12:45:45.7818	2007-04-12 12:45:47.358345	ias_surveillance_SA	IDLE	OK

© copyright 2006-2007 IP Fabrics, Inc.

2. Click on 'New' button.
3. Enter text string 'ias_surveillance_SA' into the text box.
4. Click 'OK' button.

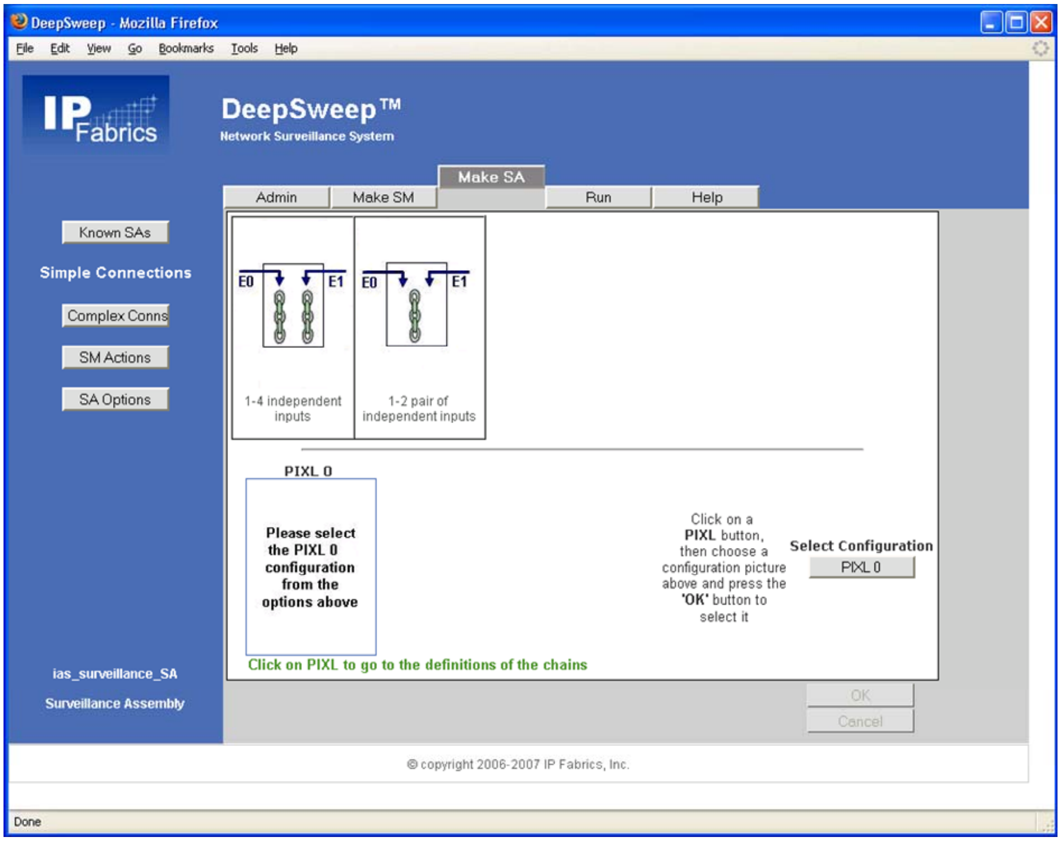

DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Admin
Make SM
Make SA
Run
Help
Known SAs
OK
Cancel
Surveillance Assembly
© copyright 2006-2007 IP Fabrics, Inc.
Done

Surveillance Assembly name: ias_surveillance_SA

This takes you to the first configuration page for this SA.

You will see the "Simple Connections" page.

[single-port example]



Please select the PIXL 0 configuration from the options above

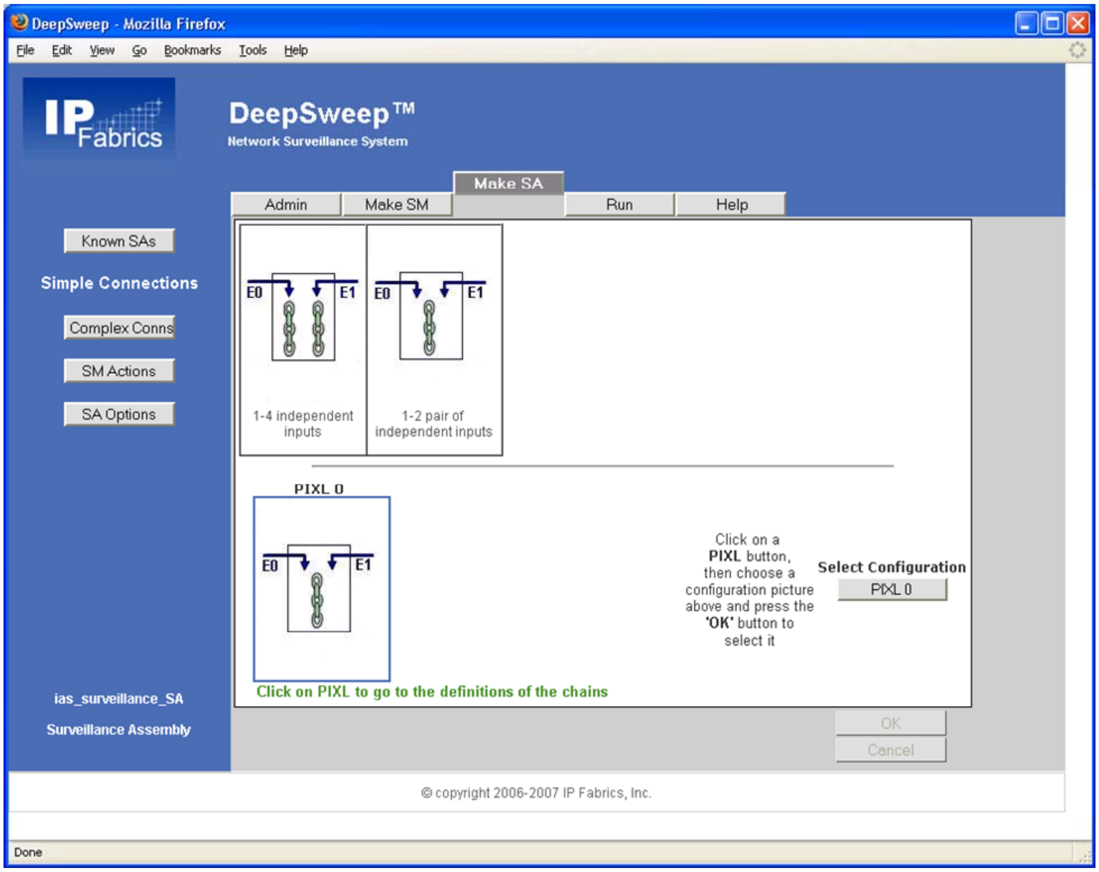
Click on a **PIXL** button, then choose a configuration picture above and press the **'OK'** button to select it

Click on PIXL to go to the definitions of the chains

Select the topology for the first PIXL (0).

5. Click button labeled "PIXL 0".
6. Click on the icon that is on the left of the set across the top. It has the descriptive text "1-4 pair of independent inputs" below it.
7. Click OK. The selected icon will appear in the definition area in the lower part of the screen.

[single-port example]



Click on a PIXL button, then choose a configuration picture above and press the 'OK' button to select it

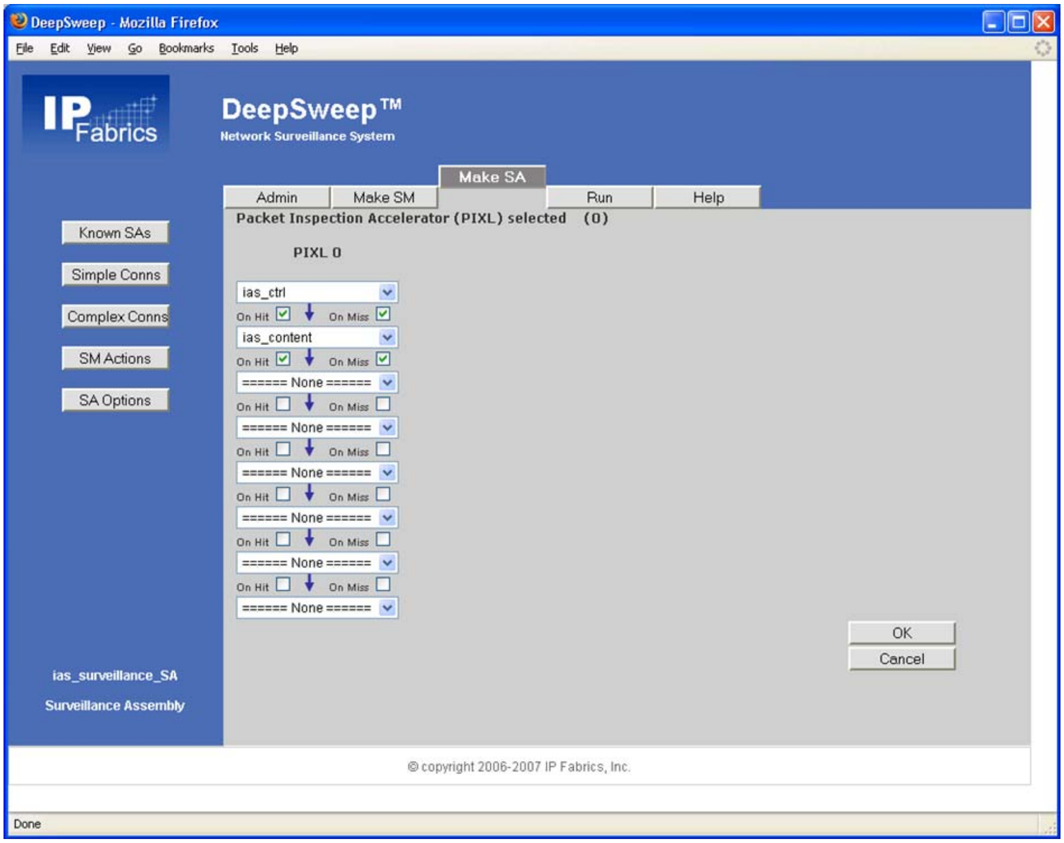
Click on PIXL to go to the definitions of the chains

© copyright 2006-2007 IP Fabrics, Inc.

Next we will place the SMs on the chain. In this case, both SMs go onto the single chain.

8. Click on the PIXL 0 chains-icon box at the lower left of the page. This will take you to the SM Chains definition page.
9. Use the drop-down menus to match the example screen image – “ias_ctrl” in the top (first) slot most chain and “ias_content” in the second slot.
10. Click OK.

[single-port example]


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Make SA
Admin
Make SM
Run
Help
Known SAs
Simple Conns
Complex Conns
SM Actions
SA Options
OK
Cancel
© copyright 2006-2007 IP Fabrics, Inc.
Done

Packet Inspection Accelerator (PIXL) selected (0)

PIXL 0

ias_ctrl
On Hit ☑ On Miss ☑
ias_content
On Hit ☑ On Miss ☑
====== None ======
On Hit □ On Miss □
====== None ======
On Hit □ On Miss □
====== None ======
On Hit □ On Miss □
====== None ======
On Hit □ On Miss □
====== None ======
On Hit □ On Miss □
====== None ======

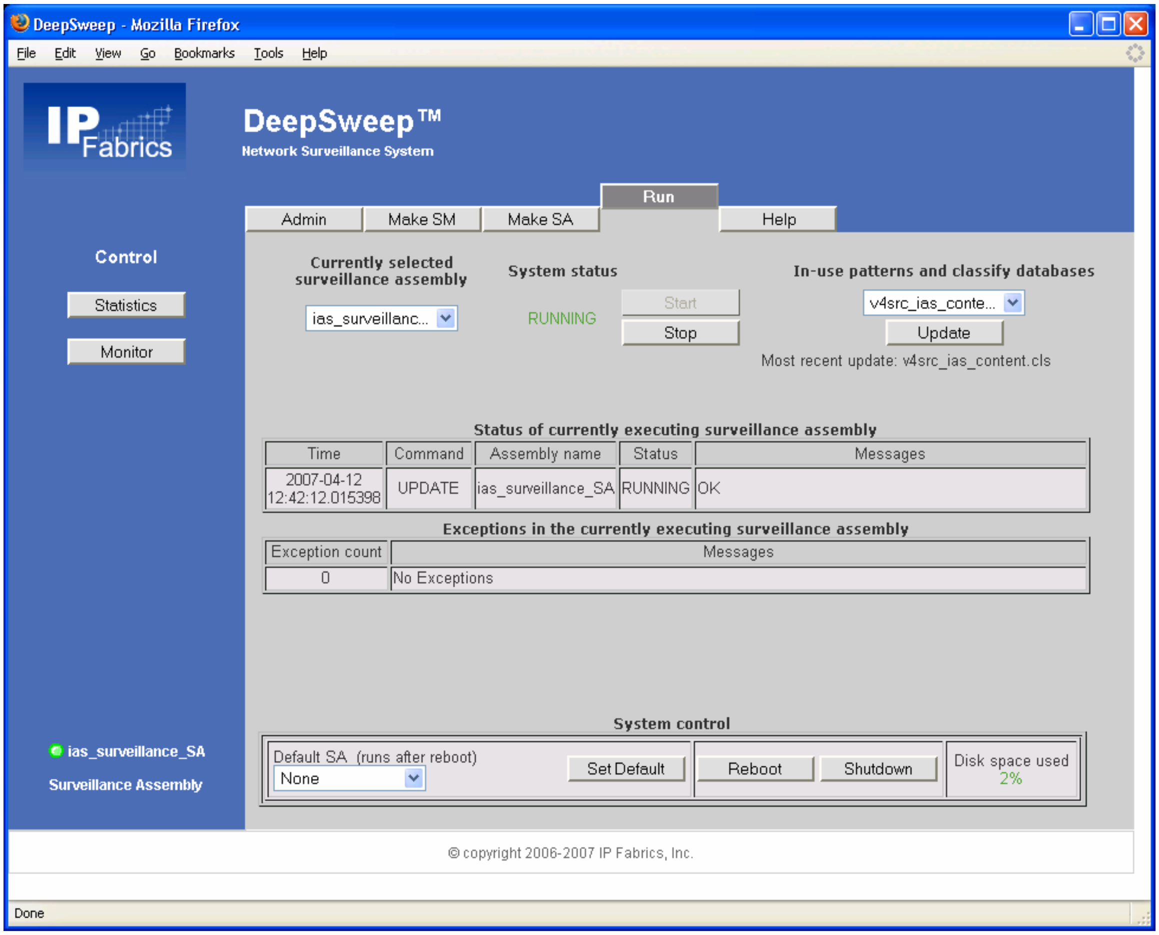
ias_surveillance_SA
Surveillance Assembly

This completes the configuration of the Surveillance Assembly. Now you are ready to RUN the SA.

Step 7: Run the ‘ias_surveillance_SA’ Surveillance Assembly

Let’s run the SA.

1. Select the ‘Run’ tab at the top of the page.
2. Select ‘ias_surveillance_SA’ from the drop-down menu on the left side of the gray area.
3. Click ‘Start’ button. You should see several changes in the Messages and Status boxes. Finally the system will display “RUNNING’ and the Messages display should show “OK”.



Currently selected surveillance assembly: ias_surveillanc...

System status: RUNNING

In-use patterns and classify databases: v4src_ias_conte...

Most recent update: v4src_ias_content.cls

Status of currently executing surveillance assembly

Time	Command	Assembly name	Status	Messages
2007-04-12 12:42:12.015398	UPDATE	ias_surveillance_SA	RUNNING	OK

Exceptions in the currently executing surveillance assembly

Exception count	Messages
0	No Exceptions

System control

Default SA (runs after reboot): None

Disk space used 2%

ias_surveillance_SA
Surveillance Assembly

© copyright 2006-2007 IP Fabrics, Inc.

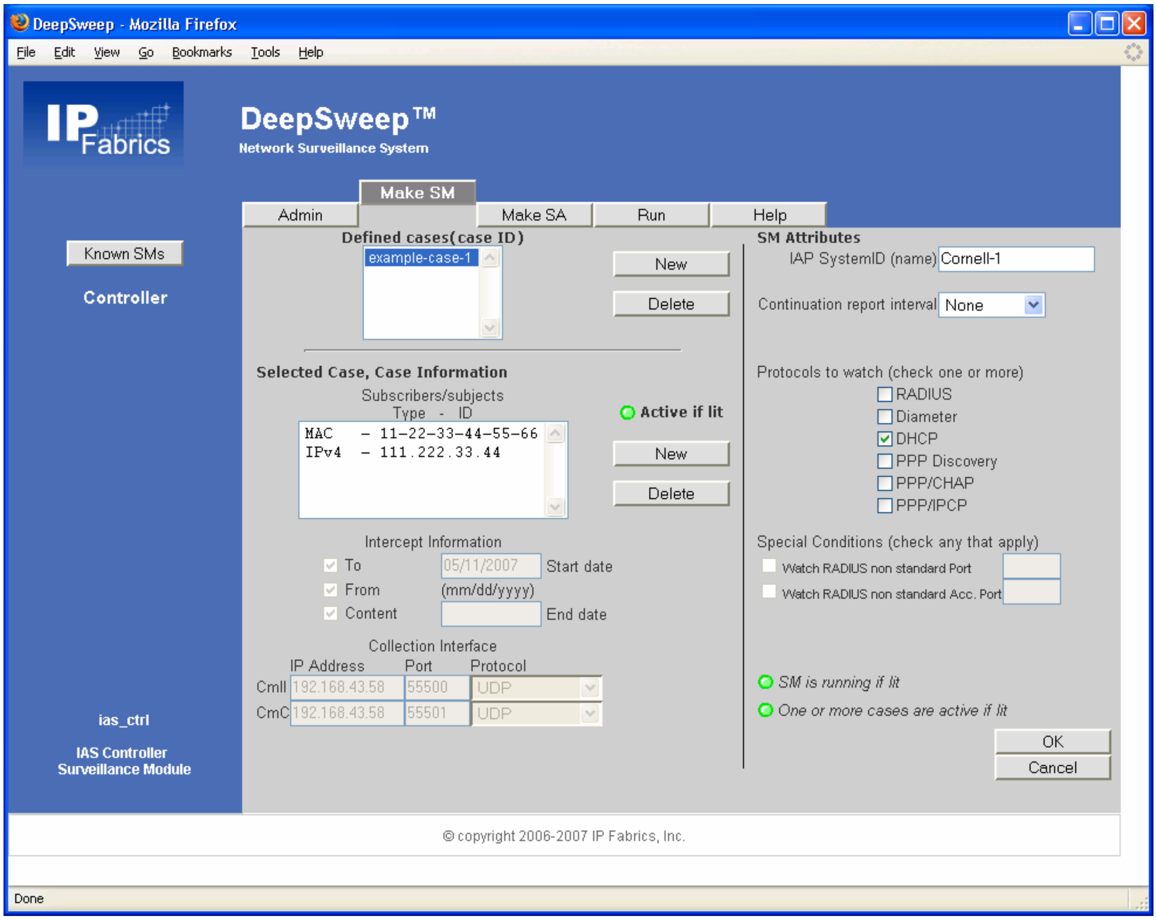
Step 8: Return to "ias_ctrl" SM

We now have a running Surveillance Assembly. If we return to the configuration page for the IAS Controller we will see some indication of this.

1. Click "Make SM" tab.
2. Select the "ias_ctrl" SM from the list.
3. Click "Edit" button.

This takes you to the IAS Controller configuration page. The SA is running so you will get an indication that this SM is alive and the one or more cases are actually running. From here, you can add new cases and/or subject IDs and they will immediately be made active if within the time window for the the start-stop dates on that case. In fact, we could have created and started the SA and then added the example case and subject IDs afterward.

4. Click on the case named example-case-1.


DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Admin
Make SM
Make SA
Run
Help
Known SMs
Controller
New
Delete
New
Delete
OK
Cancel
ias_ctrl
IAS Controller Surveillance Module
Done

Defined cases(case ID)
example-case-1

SM Attributes
IAP SystemID (name) Cornell-1
Continuation report interval None

Selected Case, Case Information

Subscribers/subjects
Type - ID

```
MAC   – 11-22-33-44-55-66
IPv4  – 111.222.33.44
```

○ Active if lit

Protocols to watch (check one or more)
☐ RADIUS
☐ Diameter
☑ DHCP
☐ PPP Discovery
☐ PPP/CHAP
☐ PPP/IPCP

Intercept Information
☑ To
☑ From
☑ Content
05/11/2007 Start date
(mm/dd/yyyy)
End date

Special Conditions (check any that apply)
☐ Watch RADIUS non standard Port
☐ Watch RADIUS non standard Acc. Port

Collection Interface

	IP Address	Port	Protocol
CmII	192.168.43.58	55500	UDP
CmC	192.168.43.58	55501	UDP

○ SM is running if lit
○ One or more cases are active if lit

© copyright 2006-2007 IP Fabrics, Inc.

Step 9: Stop the 'T1_IAS' Surveillance Assembly

To shutdown the SA click on the 'Control' button. This takes you back to the 'Run' page. Click on the 'Stop' button.

You should see the system Status go to "STOPPING' and then to 'IDLE' with the Status of 'OK'.

[NOTE: If there is an abnormally long delay with 'STOPPING' displayed then this could be due to inadvertent use of TCP in the example. Since there is probably no actual live LEA collector function at the IP address used in the example then the use of TCP is problematic.]

Step 10: Accessing data files

To access files in the user area you can use SFTP or SCP or a product such as "WinSCP" to get files after a run.

The account is 'ens_administrator' and is shipped with the default password 'ipfabrics'. See the DeepSweep User's Manual for additional details.